

Privacy Act 2020

COMES INTO
FORCE ON

1 DEC
2020

The Information Privacy Principles remain **largely unchanged**.
The key changes include:

Mandatory breach reporting

A new regime has been introduced for the mandatory reporting of a notifiable privacy breach – which is a privacy breach that causes (or is likely to cause) **serious harm**.

When assessing 'serious harm' agencies should consider factors such as: actions taken to reduce the risk of harm, the sensitivity of the affected data, the nature of harm that may be caused, the person or body that has obtained in the data.

Agencies must notify:



Office of the Privacy
Commissioner



Affected
individuals

It is an offence to fail to inform the Privacy Commissioner where there has been a notifiable privacy breach.

Offshore transfers

A new IPP has been introduced to regulate how personal information is disclosed overseas. Under the new IPP 12, an agency may only disclose personal information to a foreign entity if:

- The foreign entity is subject to privacy laws or other prescribed measures that overall provide **comparable safeguards** to those under NZ's Privacy Act; or
- The individual concerned **authorises** the disclosure (after being **expressly informed** that the information may not be subject to comparable protections).

Important: The offshore transfer requirements **do not apply** to disclosures or transfers to service providers who may hold or process personal information **solely as an agent** for another agency, provided the third party **does not use the information for its own purposes** e.g. cloud storage providers.

Criminal offences and penalties

The Privacy Act creates two new criminal offences for:

- Misleading an agency by impersonating an individual for the purpose of obtaining access to, or using, altering or destroying that individual's personal information; and
- Destroying a document containing personal information with knowledge that a request has been made in respect of that information.

The penalties for all criminal offences under the Act are increasing from \$2,000 to a fine of up to \$10,000 per conviction.

Compliance notices

The Privacy Commissioner will be empowered to issue compliance notices to agencies to require them to do something, or stop doing something, in order to comply with the Privacy Act.



Clarification to IPP1

An agency may not require identifying information from an individual unless it is **necessary for the lawful purpose** for which the information is collected.

Extraterritorial effect

All overseas agencies "carrying on business in New Zealand" will be subject to the Act regardless of:

- whether they have a legal or physical presence here;
- where the personal information is collected and held; and
- where the person to whom the personal information relates is located.



Class actions

"Aggrieved individuals", whose privacy is the subject of a complaint, investigation or proceeding may commence proceedings in the Human Rights Review Tribunal as a class. The Tribunal can award up to \$350,000 to each member of a class action.



Enforceable access directions

The Privacy Commissioner will be empowered to issue **binding directions** against agencies to allow individuals to access their information. Access directions will be enforceable by the Human Rights Review Tribunal.

Collecting personal information from children

IPP4 now emphasises that the manner of collection must be **fair** and **not intrude to an unreasonable extent** upon the personal affairs of the individual concerned, particularly where personal information is collected from children or young persons.



What's not there?

- Data portability
- Right to be forgotten
- Mandatory privacy impact assessments
- Mandatory data processing agreements
- The power for the Privacy Commissioner to issue hefty fines for non-compliance